

【特許請求の範囲】

【請求項1】 1つ又は複数のクライアント・プラットフォームと1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置であって、

(a) リモート・プラットフォームの電子的なコンテンツ又は情報に対するクライアント・プラットフォームの要求を受信し解釈し、前記要求を前記リモート・プラットフォームに送信し、データを受け取る機能、または

(b) 前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォームから受け取る機能のいずれか又は両方を行う手段を備え、

前記データは、要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービスのロケーションを表す少なくとも1つのマーカーを含んでおり、

前記装置は、前記1つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、

(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能、または

(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、

を備えるよう構成されたプロキシ・サービス提供装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般に電子権利管理に関し、特に情報技術ネットワーク環境専用の権利管理方式や他の情報操作ポリシーをサポートする柔軟なプラットフォームに関する。

【0002】

【従来の技術】 著作権は特定の種類の作品の原作者に与えられる知的所有権であり、原作者は著作権によってその作品の様々な利用法を管理できる。著作権は、文学、戯曲、音楽、美術の作品、出版物、録音物、映画（ビデオを含む）、放送（有線放送、衛星放送を含む）の原作を保護するためのものであり、著作権によって提供される権利は、保護の対象となる作品の複製、翻案、複製の配布、公演、放送などの様々な領域に及ぶ。また、多くの場合、著者には自分の作品であることを特定される権利と、自分の作品の毀損や変形に異議を唱える権利がある。さらに、録音物、映画、コンピュータ・プログラムの著作権所有者には貸与の権利が与えられるので、このような作品を公に貸し出すことによって実施するには著作権所有者から交付されたライセンスが必要になる。

【0003】 近年、録音物、文学作品、映画などのコン

テンツの電子的な保存がますます一般的になってきており、レコード店や書店などの小売店ではこのような電子コンテンツの商品流通が従来から行われている。情報技術ネットワークを介した電子コンテンツの商品流通には多くの利点があるが、このようなコンテンツの作者や流通業者に広く採用されているわけではない。その主な理由は、結果としてこのようなコンテンツをサード・パーティーが不法に複製、販売、配布しやすくなるのではないかという懸念である。このために、電子コンテンツの不当な複製を防止する技術的な防護策の開発に向けて多大な努力が払われてきた。

【0004】 デジタル・コンテンツは不法な複製が比較的容易であり、このことがコンテンツ・プロバイダにとっては好都合でもあり、不都合でもある。すなわち一方でコンテンツをできるだけ広く配布できるのは望ましいが（それによって価値が高まり、大きな利益の獲得も見込まれる）、依然として販売ごとに確実に支払いがあること、つまり著作権が侵害されないことを望んでいる。前述のような著作権侵害を防止するために、コンテンツ・プロバイダはデジタル保護方式（通常は暗号化技術に基づく）を採用する傾向がある。この方式は、a) 消費者には使いにくく配布の制限が難しい、b) 管理に費用がかかる、c) 同等のコンテンツをユーザーが操作しやすい無料の不法な方式によって無効化される恐れがある。

【0005】 既知の保護方式の1つはMicrosoft Digital Media Systemから提供されており、電子コンテンツがキーを伴って提供される。ユーザーは、正規のキー・サーバーから対応するキーを取得しないとコンテンツを再生できない。この方式の主な欠点は、ユーザーの再生装置との結び付きが強いことである。つまり、この方式で保護されたコンテンツを再生する場合は、専用の装置が必要になる。

【0006】 一般に、既知のデジタル権利管理及び保護方式には、作品の実質的な暗号化が含まれており、複製や複製されたコンテンツの再生が難しくなっている。現在使用されているデジタル権利管理（DRM: Digital rights management）技術は、ユーザーにはセキュア・コンテナとしても知られている。すなわち、この技術によって独自のファイル・フォーマットを定義し、その中で任意のメディア・ファイルをセキュアにカプセル化する。

【0007】 例えば、米国特許第6138119号に権利管理データ構造を定義、利用、操作するための技術が示されている。この明細書では、セキュアなデジタル・コンテナの概念を使用してデジタル・コンテンツの安全でセキュアな保存と転送を実現している。このようなコンテナは改ざんが難しいので、例えば、テキスト、グラフィック、実行可能ソフトウェア、オーディオやビデオなど、任意の形式のデジタル情報をパッケージ化するの

に利用できる。ただし、この方法ではセキュアなコンテンツを利用できる状況が限定される。

【0008】別のシステムでは、特定のメディア・フォーマット（Adobe（商標）PDFなど）に対して「プラグイン」セキュリティ機能を提供する。ソフトウェア・プラグイン・ビジネス・モデルは、ビデオやオーディオ（接続可能なcodec）、マルチメディア（プログラムを「拡張」する接続可能な実行プログラム）、クリエイティビティ・ツール（画像処理ツールを拡張するフィルタ）、Webブラウザなど、他の特定の市場で長年にわたってアプリケーションの拡張に使用されてきたが、現在ではAdobe Acrobat（商標）のみがセキュリティ機能を提供しており、サード・パーティーの開発者はAcrobat TMを使用して特定のフォーマットで機能するDRMを一律に開発できる。ただし、このシステムで使用方法は、ターゲット・フォーマット（PDF）の機能によって制限される。つまり、この方法ではセキュリティを保証できるフォーマットが一種類に限定され、メディアの種類が限定される。

【0009】デジタル情報製品のプロバイダ、仲介業者、消費者は、情報製作者が知的所有権（IPR）を提示し、IPRポリシー（特に卸売業者、小売業者、ライブラリなどの仲介業者が情報を操作する規則を表すポリシー）を主張する一貫したプラットフォームのない「ポリシー実施の断片化」に悩まされている。このような情報をユーザー向けに表示し、ポリシーを解釈して実施するための一貫したプラットフォームは存在しない。ネットワーク・トランザクションの途中で公表できる私的なデータの送信と再利用に関わる消費者も、やはり一貫したプラットフォームを用意してその制御下で個人的な情報を操作するポリシーを実施しているわけではない。

【0010】一般に、情報バリュー・チェーンに関わるユーザーは、操作する情報の取扱いについて要求するポリシーと受け取った情報の取扱い又は処理についてのポリシーを提示してから情報を受け取ることを希望している。既知の技術では、この問題を一貫した体系的な方法で解決することはできない。

【0011】コンテンツのフィルタリングと適応のためにプロキシ・サービスを利用するという概念が知られている（「プロキシ」は、広義では単に「代理に付与された権限」を意味する）。例えば、望ましくないコンテンツの広告などを除去するための規則に基づくフィルタリングは、新たに発生した作業である。特に米国特許第5,996,011号では、ネットワークを介してコンピュータが受け取るデータから特定のデータをフィルタで除去することによって、受け取ったデータへのアクセスを制限するシステム及び方法について記述している。1つの実施態様では、インターネットに接続されたコンピュータが受け取るWorld Wide Webページ

から好ましくないテキスト・データ又は対象となるテキスト・データをフィルタリングするコンピュータベースの方法が示されている。米国特許第6,119,165号には、インターネット又はインターネット環境において、多くのクライアントをサポートするプロキシ・サーバーに機能を追加し、クライアントの特性に基づいて特定のクライアントにソフトウェア・モジュールを提供できるようにするシステムに関する記述がある。こうしてダウンロードされたモジュールは、プロキシ・サーバーとクライアントとの双方向通信リンクをセットアップしたクライアントによって実行される。双方向リンクによって、例えばクライアント・プラットフォームのウィンドウを使用したクライアント側でのステータス表示が可能になり、ウィルス・スキャン、コンテンツのフィルタリング、帯域幅利用など、プロキシ・サーバーの現在のステータスを表示できる。他のアプリケーションでは、ダウンロードされたモジュールによって組織の掲示板、ニュース・チャンネル、一般的なソフトウェア・パッチの提供元を構築できる。

【0012】米国特許第5,987,606号には、インターネット・コンピュータ・ネットワークからリモート・インターネット・サービス・プロバイダのサーバーによって取得され、ローカル・クライアント・コンピュータに転送されるインターネット・コンテンツをフィルタリングするシステムが示されている。このシステムでは、包含的なフィルタや排他的なフィルタなどの少なくとも1つのフィルタリング方式と、許可されるサイト又は除外されるサイトのリストなどの少なくとも1つのフィルタリング要素をローカル・クライアント・コンピュータで生成された個々のインターネット要求と照合する。この場合はISPサーバーにフィルタリング方式が実装されているが、一般にこの種のフィルタリング・サービスや適応サービスはクライアント側、サーバー、両者の中間点のいずれに適用してもよい。さらに、フィルタリングと適応はダウンストリーム・コンテンツ（クライアント・プラットフォームがサーバーから受け取るコンテンツ）に限定する必要はない。つまり、プライバシーや匿名を保証するためにユーザー入力に適応するプロキシ・サービスが存在する。

【0013】

【発明が解決しようとする課題】ただし、既知のプロキシ・サービスはいずれも情報操作ポリシーの適用（特に著作権の管理と行使のサービス）の実践的な介入ポイントを提供しない。前述のとおり、一般に著作権ポリシーを実施する既知のメカニズムでは、通常クライアント側で特別な「読み出し」ソフトウェアを使用し、コンテンツに関するエンドユーザーの楽しみを損なう結果になるか、サーバー側で非常に限定的なコンテンツに依存するポリシー実施機能を使用し、エンドユーザが鑑賞できるコンテンツを制限してしまうことになる。専用のクライ

アント・アプリケーションには、プラットフォーム互換性やアプリケーション互換性による制限からユーザーの不便まで、多くの欠点がある。既知のサーバーベースのシステムにも、管理上の粒状性の問題からコンテンツの柔軟性の問題まで、多くの弱点がある。

【0014】

【課題を解決するための手段】そこで、以上の問題を克服するための仕組みを考案した。こうして、本発明の第1の側面に従って、1つ又は複数のクライアント・プラットフォームと電子的なコンテンツ又は情報を提供する1つ又は複数のリモート・コンテンツ・プロバイダの間のプロキシ・サービスを提供する装置が提供される。

【0015】この装置は、コンテンツ・プロバイダの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈する手段と、前記要求をコンテンツ・プロバイダに送信し、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含むデータを受け取る手段と、前記1つ又は複数のマーカを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信する手段を備えている。

【0016】また、本発明の第1の側面に従って、1つ又は複数のクライアント・プラットフォームと電子コンテンツを提供する1つ又は複数のリモート・コンテンツ・サーバーの間のプロキシ・サービスを提供する方法も提供される。本方法には、コンテンツ・サーバーの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈するステップと、前記要求をコンテンツ・サーバーに送信するステップと、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含むデータを受け取るステップと、前記1つ又は複数のマーカを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信するステップが含まれる。

【0017】本発明の第2の側面に従って、1つ又は複数のクライアント・プラットフォームと前記1つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置が提供される。本装置は、リモート・プラットフォームに送信するデータが前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリシ

ー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含んでいる場合に、前記データをクライアント・プラットフォームから受け取る手段と、前記1つ又は複数のマーカを解釈する手段と、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する手段を備えている。

【0018】さらに、本発明の第2の側面に従って、1つ又は複数のクライアント・プラットフォームと前記1つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する方法も提供される。本方法には、リモート・プラットフォームに送信するデータがリモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含む場合に、前記データをクライアント・プラットフォームから受け取るステップと、前記1つ又は複数のマーカを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信するステップが含まれる。

【0019】このようにして、本発明はクライアント・プラットフォームと様々な権利管理ポリシーや情報操作ポリシーを伴う様々なコンテンツ・プロバイダとの中継点として利用できるプロキシ・サービスを提供し、それによってコンテンツ・プロバイダは自社の独自のポリシーを確実に実施できる。従って、本発明はクライアント・プラットフォームとクライアント・プラットフォームが機密性の高い情報や個人的な情報を送信する様々なリモート・ロケーションとの中継点として利用できるプロキシ・サービスを提供し、それによってクライアント・プラットフォームの機密性／匿名性に関する独自のポリシーを確実に維持できる。本発明に従った1つのプロキシ・サービスは2つの目的で利用できる。つまり、このようなサービスはクライアント・プラットフォームから受信するデータとクライアント・プラットフォームに送信するデータの両方を処理するように調整できる。

【0020】本プロキシ・サービスは、クライアント・プラットフォーム上にローカルに配置してもよい。ただし、「クライアント」が複数のプラットフォームを含む組織的なネットワークを備える場合は、本プロキシ・サービスをそのネットワーク内の中心に配置してもよい。あるいは、本プロキシ・サーバーをインターネットなどの情報技術ネットワークのリモート・ポイントに配置してもよい。

【0021】コンテンツ・サーバーは、本プロキシ・サービスからのコンテンツ要求に応答して1つ又は複数のマーカーを含むデータ・ストリームを返す。マーカーには、プロキシ・サービスがクライアント・プラットフォームにコンテンツの複製を送信する前に対話する必要がある他の1つ又は複数のサービスのロケーションの詳細情報（URLやDOIなど）が含まれる。このようなマーカーはデータ・ストリームに埋め込まれており、これを認識でき、解釈できるのはプロキシ・サービスの内部で提供される専用の手段に限定されるのが好ましい。

【0022】クライアント・プラットフォームがWebブラウザなどの場合は、情報操作／権利管理リモート・サーバーにコンテンツ要求を送信する際に（直接又は間接的に）、プロキシ・サービスは要求内にクライアント・プラットフォームに関連するデータ（セッションIDなど）を含むように調整されているのが好ましい。従って、情報操作／権利管理リモート・サーバーにクライアント・プラットフォームに関する情報が提供される。要求には、エンド・ユーザーに固有の詳細情報を含めることもできる（特に、エンド・ユーザーとクライアント・プラットフォームが別のエンティティであり、エンド・ユーザーとクライアント・プラットフォームが対話するための情報操作／権利管理サーバーに関連する特別な要件がない場合）。

【0023】情報操作／権利管理サーバーがプロキシ・サービスからコンテンツ要求を受信し、要求の合法性を検証すると、情報操作／権利管理サーバーはコンテンツのクリア・コンテンツ・バージョンを作成し、これをローカル又はリモートの特定のロケーションに保存し（できれば一時的に）、さらに前記ロケーションの詳細情報をプロキシ・サービスに返す。プロキシ・サービスは、コンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォームのロケーションの詳細情報を送信するように調整できるのが好ましい。このことによって、情報操作／権利管理サーバーに関する特定の要件が満足された場合に、クライアント・プラットフォームは前記クリア・コンテンツの複製を取得できる。

【0024】情報操作／権利管理サーバーが採用するポリシーがコンテンツ・プロバイダと（当然のことながら）要求されたコンテンツの性質に依存するのは言うまでもない。情報操作／権利管理サービスがクライアント・プラットフォーム又はエンド・ユーザーに関連付けできることも明らかである。このことによって、クライアント・プラットフォームからリモート・ロケーションに送信される情報をプロキシ・サーバーによって操作し、適切な情報操作サービスを介して処理してから、前記リモート・ロケーションに送信できる。

【0025】

【発明の実施の形態】ここで、単に例として添付の図面

を参照しながら本発明の1つの実施態様について説明する。

【0026】図1を参照すると、Webブラウザ10（クライアント・コンピュータ・プラットフォーム（図示せず）からアクセス可能）、本発明に従ったプロキシ・サーバー12、デジタル権利管理（DRM）Webサービス14の間の典型的な接続（1つの例）が示されている。この接続は、通常はインターネットなどの情報技術ネットワークを介して行われる。矢印1、2、2a、3、3a、4、4a、4b、4c、4d、5、6、7は、以下に記述する典型的なプロセスでWebブラウザ10、プロキシ・サーバー12、DRM Webサービス14の間でやりとりする要求や応答の方向を示している。

【0027】最初のインスタンスでは、固有のセッションIDが生成された時点でWebブラウザ10がプロキシ・サーバー12にログインする。セッションIDはエンド・ユーザーには認識されず、後のプロセスでセッションの検証に使用される。

【0028】矢印1を参照すると、表示側クライアントすなわちWebブラウザ10はプロキシ・サーバー12にネットワーク・アドレス（例えばURLやDOI）を提示することでネットワーク・リソースの要求を行う。プロキシ・サーバー12は、ユーザーのワークステーションにローカルにも、企業や組織のネットワークに集中的にも、あるいはインターネットなどの情報技術ネットワークのリモート・ポイントにも配置できるのは言うまでもない。

【0029】プロキシ・サーバー12は、通常は、HTTPプロトコルを使用して、コンテンツ・サーバー16にリソースへの適切なネットワーク要求を送信する（矢印2）。コンテンツ・サーバー16は、通常はプロキシ・サーバー12とは別のロケーションに存在し、Webページなどのリソースを返す（矢印2a）。リソースは、一般にHTMLファイル又はより一般的なXMLファイルの形式をとる。リソース・ファイルには、他のリソースを呼び出すマークアップ・タグに類するものが埋め込まれており、プロキシ・サーバー12が提供する情報操作ポリシー又はデジタル権利管理に従った専用の処理のみによって取得できる。本発明のこの実施態様では、この種のマークアップ・タグは<DRM>オブジェクトとして記述される。プロキシ・サーバー12に送信される他の「オープン」なデータ・ストリーム内のこのような<DRM>オブジェクト・インスタンスは、プロキシ・サーバー12が埋め込みコンテンツ・オブジェクトのクリア（すなわち暗号化されていない）バージョンのロケーションを確認するために対話する必要がある他のWebリソースを参照する属性（URLやDOIなど）を備えている。

【0030】コンテンツ・サーバー16から受け取った

データ・ストリーム内に埋め込まれたマークアップ・タグにプロキシ・サーバー12が適応するのは言うまでもない。最初にプロキシ・サーバー12を通過することなくWebブラウザ10がコンテンツ・サーバー16から直接データ・ストリームを取得しようとしても、ブラウザが認識できるのはストリームの「オープン」な部分のみである。従って、マークアップ・タグを認識も解釈もできない（つまりWebブラウザ10はタグを無視する）。

【0031】プロキシ・サーバー12はコンテンツ・サーバー16からリソース・データ・ストリームを受け取ると、生成された一連の規則に従って受信したストリームを確認し、データ・ストリームに埋め込まれた1つ又は複数のマークアップ・タグを検出する。プロキシ・サーバー12は、例えばインターネット上のリモート・ポイントに配置された「drmファイル」のロケーションを示すプロパティをタグ本文から抽出するように調整されている。次に、プロキシ・サーバー12は指定された<DRM>ファイル（1つ以上）を要求し（矢印3）、受信する（矢印3a）。<DRM>ファイルでは、例えばXML構文を使用してもよい。プロキシ・サーバー12は、このファイルから実際のコンテンツ・オブジェクト（通常はセキュア・コンテナなどにパッケージ化されている）の“content_type”と“content_location”（例えばURL）を抽出する。

【0032】このサービスは、通常は“MIME”エンコード（image/jpegなど）を使用したcontent_typeを解釈し、このcontent_typeをプロキシ・サービスに登録した1つ又は複数のcontent_typeと比較する。content_typeがサービスに登録されたタイプの1つであれば、エンド・ユーザーに返す「クリア」なタグ構造が決定する。例えば、パッケージ化されたコンテンツがMIMEタイプ・イメージ/jpegの場合、変更されたタグ構造は“”のフォーマットでなければならない。つまり、エンド・ユーザーが（例えば登録ユーザーやライセンスを付与されたユーザーとして）リソースを使用できるようにする場合、プロキシ・サーバー12は次のように動作する。

【0033】ここで、プロキシ・サーバー12は、リモートDRM Webサービス14が指定されたリソースのセッションに固有の「クリアコンテンツ」バージョンを作成し、セッションに固有のURLを返すことを要求する（矢印4）。詳しく記述すると、drmサービス・インターフェイス18は<drm>ファイルの暗号化バージョンをdrm Webサービス14内の暗号化コンテンツ・アーカイブ20に配置する（矢印4a）。次に、コンテンツ・アーカイブ20は暗号化された<drm>ファイルを、やはりdrm Webサービス14内

に存在する解読コンポーネント22に送信する。解読コンポーネント22は、ファイルを解読してその「クリアコンテンツ」バージョンを作成する。このクリアコンテンツ・バージョンは、セッションに固有の（一時的な）固有のファイル名を使用して、やはりdrm Webサービス14内に存在するクリアコンテンツ・キャッシュ24に送信され（矢印4c）、キャッシングされる。また、固有のファイル名はdrmサービス・インターフェイス18に送信され、セキュアでないリソースのセッション固有のURLを生成してプロキシ・サーバー12に送信する（矢印4d）。

【0034】プロキシ・サーバー12は、（この場合は）MIME対応のフォーマットを使用して変更されたコンテンツ・ストリーム（例えばHTMLページ）を作成する。HTMLページは、drm Webサービス14が提供するセッション固有の一意のURLを特定するように再フォーマットされる。再フォーマットされたHTMLページは、ここでWebブラウザ10に返される（矢印5）。

【0035】次に、Webブラウザ10はdrm Webサービス14内のクリアコンテンツ・キャッシュ24にリダイレクタ・サービス・インターフェイス26を介して保存されるセキュアでないコンテンツを要求する（矢印6）。ブラウザの要求は、現在のブラウザ・セッションのみで有効なセッション固有のURLを含むクエリー・ストリングで構成される。リダイレクタ・サービス・インターフェイス26は、現在のブラウザ・セッションを確認してブラウザ10が送信するクエリー・ストリングに記述されるセッション固有のURLと比較する。セッションが一致し、クリア・コンテンツの一時記憶にタイムアウト規則があればその期限が切れていない場合に、リダイレクタ・サービス・インターフェイス26はWebブラウザ10にクリア・コンテンツを送信し、エンド・ユーザーはこれを利用できるようになる。

【0036】本発明は、プロキシベースの介入とコンテンツの適応という新しい概念に基づいており、情報操作ポリシーとデジタル権利管理ポリシーの解釈と実施を総括するプラットフォームを提供する。これは、特にポータルなどの場合に有効である。このような状況では、ユーザーが様々な表示環境を使用する関連の大規模なベースに対して、一貫した柔軟な方法でポリシーを適用する必要がある。換言すれば、本発明を使用すると、組織の異機種ネットワーク上にユーザー固有の情報操作ポリシー（著作権行使のポリシーなど）を一貫して適用できる。

【0037】本発明で採用する手法では、本質的にユーザー認証及び認可のプロセスとメカニズムをポリシー実施の実際の実装とは別に維持している。このことによって、組織又はコンテンツ・サービスは集中管理の企業データベースを利用して情報ポリシー（電子ジャーナルに

関する組織のサイト・ライセンスなど、特に組織内の様々なロールに様々なポリシーが適用される場合)を管理できる。

【0038】明細書の以上の部分では、本発明についてその特定の典型的な実施態様に関連して記述してきた。ただし、前述の請求項に示す本発明の精神と範囲を逸脱しない限り、その様々な変形や変更が可能なことは、当業者には明らかである。従って、本明細書と図面は制限を意味するものではなく例示を意図するものと見なす必要がある。

【0039】この発明は、例として次の実施形態を含む。

【0040】(1) 1つ又は複数のクライアント・プラットフォーム(10)と1つ又は複数のリモート・プラットフォーム(16)の間のプロキシ・サービス(12)を提供する装置であって、(a) リモート・プラットフォーム(16)の電子的なコンテンツ又は情報に対するクライアント・プラットフォーム(10)の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム(16)に送信してデータを受け取る機能、または(b) 前記リモート・プラットフォーム(16)に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム(10)から受け取る機能のいずれか又は両方を行う手段を備えており、前記データは要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス(14)のロケーションを表す少なくとも1つのマーカを含んでおり、前記装置は、前記1つ又は複数のマーカを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能と、(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、を備える前記装置。

【0041】(2) プロキシ・サービス(14)による情報又はコンテンツの要求に回答して1つ又は複数のマーカを含むデータ・ストリームを返し、マーカにはプロキシ・サービス(12)がクライアント・プラットフォーム(10)にコンテンツの複製を送信する前に対話する必要がある他の1つ又は複数のサービスのロケーションの詳細情報が含まれる(1)に記載の装置。

【0042】(3) データ・ストリームにマーカが埋め込まれており、プロキシ・サービス(12)の内部で提供される専用の手段のみによってマーカを認識でき、解釈できる(2)に記載の装置。

【0043】(4) クライアント・プラットフォームが

Webブラウザ(10)などの場合、情報操作／権利管理リモート・サービス(14)に情報又はコンテンツ要求を送信する際に、プロキシ・サービス(12)が要求内にセッションIDなどのクライアント・プラットフォーム(10)に関連するデータを含むように調整される(1)から(4)のいずれかに記載の装置。

【0044】(5) 情報操作／権利管理サービス(14)がプロキシ・サービス(12)からコンテンツ要求を受信して要求の合法性を検証すると、コンテンツのクリア・コンテンツ・バージョンを作成し、ローカル又はリモートの特定のロケーション(24)に保存し、さらに前記ロケーションの詳細情報をプロキシ・サービス(12)に返す(1)から(4)のいずれかに記載の装置。

【0045】(6) 前記コンテンツのクリア・コンテンツ・バージョンが一時的に記憶される(5)に記載の装置。

【0046】(7) プロキシ・サービス(12)がコンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォーム(10)のロケーションの詳細情報を送信するように調整され、その結果、情報操作／権利管理サービス(14)に関する特定の要件が満足された場合にクライアント・プラットフォーム(10)が前記クリア・コンテンツの複製を取得できる(5)に記載の装置。

【0047】(8) 1つ又は複数のクライアント・プラットフォーム(10)と1つ又は複数のリモート・プラットフォーム(16)の間のプロキシ・サービス(12)を提供する方法であって、(a) リモート・プラットフォーム(16)の電子的な情報又はコンテンツに対するクライアント・プラットフォーム(10)の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム(16)に送信してデータを受け取るステップと、(b) 前記リモート・プラットフォーム(16)に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム(10)から受け取るステップのいずれか又は両方を含み、前記データに要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス(14)のロケーションを表す少なくとも1つのマーカが含まれており、さらに前記1つ又は複数のマーカを解釈するステップと、情報操作／ポリシー実施のサービス(12)の要件が満足された場合に、(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォーム(10)に提供するという要求を前記クライアント・プラットフォーム(10)に代わって送信するステップと、(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・プラットフォーム(16)に提供するという要求を適切な情報操作ポリシー実施サービス(12)に送信するステッ

14

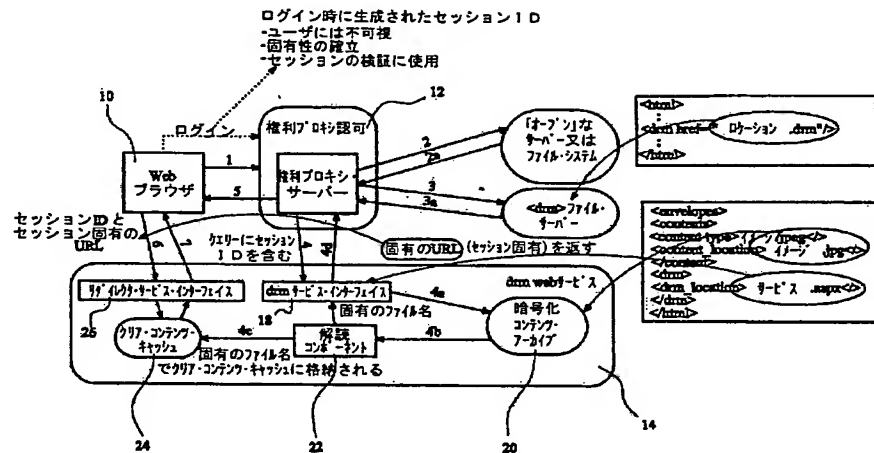
10 クライアント・プラットフォーム

12 プロキシ・サービス

14 情報操作／権利管理リモート・サービス

16 リモート・プラットフォーム

【图 1】



フロントページの続き

Fターム(参考) 5B017 AA07 BA06 CA16
5B085 AA08 AE02 AE23 BA07 BC02
BE04 BG04 BG07